The Internet and privacy

The Internet and Privacy: When Can Universal Human Rights be Violated?"

There has been much discussion, over the last few years, about the impact of the widespread use of computers on people's privacy. The rapid growth of the Internet as a tool of trade, research, and entertainment, has only served to intensify that discussion. Much of the discussion of privacy on the Internet has focussed on legal conceptions of what the right to privacy might entail, and thus deals primarily with the issue of what legal protection users of the Internet (particularly American users of the Internet) might be entitled to. Such an approach seems to me to be somewhat wrong-headed, and so in this paper I want to look at this problem in a different way. I hope to achieve three main aims: (1) to highlight the problems involved in discussing an essentially philosophical question within a legal framework, and thus to show that providing purely legal answers to an ethical question is an inadequate approach to the problem of privacy on the Internet; (2) to discuss what privacy in the medium of the Internet actually is; and finally (3) to attempt to apply a globally acceptable ethical approach to the problem of privacy on the Internet, and thus to answer the question of what is and is not morally permissible in this area.

Introduction

There has been much discussion, over the last few years, about the impact of the widespread use of computers on people's privacy. The rapid growth of the Internet as a tool of trade, research, and entertainment, has only served to intensify that discussion. Much of the discussion of privacy on the Internet has focussed on legal conceptions of what the right to privacy might entail, and thus deals primarily with the issue of what legal protection users of the Internet (particularly American users of the Internet) might be entitled to.

Such an approach seems to me to be somewhat wrong-headed, and so in this paper I want to look at this problem in a different way. I hope to achieve three main aims: (1) to highlight the problems involved in discussing an essentially philosophical question within a legal framework, and thus to show that providing purely legal answers to an ethical question is an inadequate approach to the problem of privacy on the Internet; (2) to discuss what privacy in the medium of the Internet actually is; and finally (3) to attempt to apply a globally acceptable ethical approach to the problem of privacy on the Internet, and thus to answer the question of what is and is not morally permissible in this area.

I should make it clear from the start that I am taking a very broad view of the entire issue of privacy on the Internet, and so I expect the points that I make in this discussion will apply to a wide range of Internet practices. Some specific practices will be mentioned during the course of the paper, and I hope that by the end of this paper I will have dealt with the privacy issues raised by all the specific practices that I mention.

The Legal Approach to Privacy on the Internet

In investigating the issue of privacy on the Internet, one common approach has been to focus on legal principles that apply in certain situations in the real world, and then to attempt to apply these same principles to the virtual world. While some of these discussions have focussed purely on legal issues that may arise out of apparent breaches of privacy on the Internet, others have attempted to draw ethical conclusions out of the legal principles that are examined.

An example of this is the work of Robert McArthur, who has taken the concept of "reasonable expectation of privacy" from the real world, and then used this principle to examine two forms of Internet activity; browsing the World Wide Web, and sending and receiving e-mail.[1] McArthur suggests that there are two essential principles against which any apparent breach of privacy in the real world must be judged, and if either one of these two principles apply, then there has been no **legal** breach of privacy. McArthur calls these the "Mischance Principle" and the "Voluntary Principle".

The Mischance Principle – we cannot reasonably expect to maintain privacy over that which another person could discover, overhear, or come to know without concerted effort on his/her part to obtain this information.[2]

---

[1] Robert McArthur "Reasonable Expectations of Privacy" *Ethics and Information Technology* 3(2001)123-128.

[2] Ibid. p. 124. McArthur attributes the original discussion of this principle to Mark Tunik *Practices and Principles* (Princeton University: Princeton, 1998) pp. 161-190.

The Voluntary Principle – If I choose to decrease the relative amount of privacy for myself and information under my control by exposing it to view, I thereby decrease the reasonableness of any expectation that this privacy will be observed.[3]

In his discussion of browsing the World Wide Web, McArthur suggests that since it is now widely known that the one's web browsing history can be tracked through the use of cookies and other software, browsing the World Wide Web is essentially a public activity, and thus falls foul of the Voluntary Principle. Unless I take specific measures to conceal my identity or to block the tracking software, then I have chosen to reveal this information about myself. Thus it is, legally speaking, unreasonable to expect privacy in this domain and it is not a breach of my privacy for someone to collect this click-stream data.

In his discussion of sending and receiving e-mail, McArthur suggests that it is common knowledge that this medium of communication is not secure. As evidence of this he points to the fact that many major companies have put in place programs to monitor their employees' e-mail,[4] that many e-mail messages are erroneously intercepted by the technology that is employed by law enforcement agencies to intercept the e-mail of suspected criminals,[5] that backup tapes that may contain e-mails are not securely stored, and so on. McArthur again draws on the Voluntary Principle to assert that it is unreasonable to expect privacy in e-mail; if I entrust material to an e-mail while knowing that the global e-mail system is not secure, then I have chosen to reveal this information, and my privacy has not been breached if the material in that e-mail becomes public.

The biggest problem with a discussion like this is that it is based on what is actually true at the present time; on what is the case. While it is of some interest to know what the law

---

[3] Ibid. pp. 124-125.

[4] Ibid. p. 127 – drawing on a report from the American Manufacturing Association, www.amanet.org/press/research/checkemail.

[5] Ibid. McArthur quotes *Electronic Privacy Information Center Alert* 7.15, August 3, 2000 (www.epic.org/alert/EPIC_ALERT_7.15.html).

does and does not allow, in discussions such as this we are generally far more interested in what **ought** to be the case, rather than what **is** the case. And discussions of law are almost invariably discussion about what is, rather than about what ought to be. In discussing the transfer of child pornography through the Internet, for example, while it may be of interest to know what laws would apply to those engaged in the practice, the main reason that this is of interest is because of an already formed a moral judgement; that engaging in the trade of child pornography is wrong, and thus the interest in what laws might apply is actually an interest in preventing the trade of child pornography through the Internet. If it was to turn out that there were no laws that applied to the trade of this material, then it is likely that there would be a call for laws to be passed that would ban the trade of child pornography on the Internet. Criminal laws that apply to the dealings on the Internet have their base in moral principles, as in fact do all criminal laws. It is because of a prior moral judgement, that engaging in a particular action is wrong, that criminal laws are established in the first place.

Thus in examining the issue of privacy in the use of computers, and privacy on the Internet, the primary interest is always likely to be in a moral issue, about what is the right and wrong thing to do, rather than in a legal issue, about what is legal and illegal. So while it may be true that e-mail, for example, is not a fully secure communication medium, that is a statement about what is the case, and not about what ought to be the case. McArthur points out that many companies monitor the e-mail of their employees, and that law enforcement agencies may intercept innocent e-mails while attempting to intercept the e-mail of criminals. This may well be true, but it does not even attempt to answer the question of whether companies **ought** to monitor employees' e-mail, or whether law enforcement agencies **ought** to try to intercept e-mail sent by suspected criminals. Similarly, the fact that one's Internet browsing habits may be recorded by software placed on websites and downloaded on to the browser's computer, does not answer the question of whether such software **ought** to be placed on websites.

While there are some extremely worthwhile points raised in discussions of the legal

issues of privacy, I hope that this discussion has shown that a legally based discussion cannot answer the fundamental ethical questions raised by the issue of privacy and the Internet. To attempt to answer such questions it is necessary to determine what ought to be the case, rather than what is the case. In order to answer that question, it will be necessary to examine the concept of privacy, and to attempt to come to some understanding of why privacy is an ethically important concept, and thus how questions of privacy on the Internet ought to be addressed.

What is Privacy?

Defining privacy is, unfortunately, not an easy task. There are innumerable definitions of privacy as a philosophical concept, and while most will capture some important aspects of the issue, it is virtually impossible to arrive at a definition that is not flawed in some way. Privacy as a concept is most commonly discussed as a right possessed by persons, and it is definitions of the right to privacy that are generally considered to be the most philosophically important. For example, an early, and extremely influential definition of the right to privacy was formulated by Warren and Brandeis,[6] who suggested that the right to privacy was "the right to be left alone",[7] to protect the privacy of one's thoughts and emotions. Warren and Brandeis saw this as one important aspect of a broader interest in being left alone to pursue one's own projects; in other words, they derived a right to privacy from a broader right to liberty. One problem with such a definition is the fact that a person's privacy can be invaded without any direct infringement of their liberty.[8] Another problem is that conceiving of a right to privacy in this way makes the right too broad, and gives no clues as to when such a right might be justifiably overridden.[9]

Another way of defining the right to privacy is in terms of a right to control access to

---

[6] Samuel Warren and Louis Brandeis, "The Right to Privacy" *Harvard Law Review* (1890) cited in Lisa Austin "Privacy and the Question of Technology" *Law and Philosophy* 22(2003)119-166. pp. 121-123.

[7] Warren and Brandeis, quoted in Austin. Ibid.

[8] See Darren Charters "Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience" *Journal of Business Ethics* 35(2002)243-254. pp. 246-247.

[9] Ibid.

one's personal information.[10] Seeing privacy in this way makes it akin to a property right, in that it can be dealt with in any way that the owner wishes. However, it is questionable whether it is appropriate to link privacy and control in this way, since this definition is open to a counter-example. A person who freely discloses intimate information about themselves to a wide range of people has suffered a loss of privacy, but since the disclosure of that information was entirely voluntary, there has been no loss of control. It seems clear that some sense of control of personal information is an important aspect of privacy, but it cannot constitute privacy in and of itself.

A third way to define privacy is to make reference to the notion of public and private spheres of life. The private sphere is that part of life concerned with familial, personal, and intimate relations, while the public sphere is the part of life concerned with action in the community. This is the way that the terms are used in business, for example when discussing public sector and private sector enterprises. If privacy is taken as referring to the private realm, then a right to privacy is simply a right to ensure that one's life is not subject to undue interference from the government. While defining privacy in this way does capture some important ideas, it falls far short of an adequate definition of privacy generally, for such a definition would suggest that it is only the government and its agencies that can infringe upon a person's privacy, which is clearly not the case.

While there are clearly problems with the main definitions of privacy, it is also the case that these influential definitions each manage to delineate some important aspect of privacy. Warren and Brandeis highlight the necessity of privacy in order to allow a person to pursue their own life goals and projects.[11] Accounts that link privacy to control over the release of personal information, draw attention to the fact that a right to privacy is necessary (at least in some cases) in order to prevent a person from being harmed. For example, if a person's sexual preferences were considered to be socially unacceptable,

---

[10] Ibid. Charters draws heavily on the work of H. McCloskey "Privacy and the Right to Privacy" *Philosophy* 55(1980)17-38.

[11] Warren and Brandeis "The Right to Privacy".

then that person might be harmed if that information was to become widespread. Thus a right to control the release of this personal information is necessary to prevent harm to that person. Accounts of privacy that draw a distinction between the public and the private aspects of a person's life serve as a reminder of the importance of this distinction, for if there is excessive interference of the government into the private domain, then certain public roles become impossible to fulfil. An example of this is the necessity for secret ballots in elections; if a person's voting preferences are known to the government, then it becomes difficult (if not impossible) for that person to properly fulfil their public role as a voter. Thus it can be seen that while it may not be easy to arrive at a precise definition of privacy, it is possible to sketch out the main features of a right to privacy.

What aspects or features of life must a right to privacy protect? Three things have already been mentioned. A right to privacy must be, in at least some sense, a right to be left alone, and a right to exclude others, which would include a right to not be subject to unjustified surveillance. A right to privacy must also allow a person to control, at least to some extent, the release of personal information about themselves. A right to privacy must also protect a person from unjustified interference by the government, lest one's public roles be undermined.

The extent to which a right to privacy can limit these sorts of violations of privacy is also a source of some debate. For example, the question of the control of the release of personal information has been debated at some length. Some people have argued that virtually all information about a person is public information, which thus makes that information available for publication and dissemination. Others suggest that even information about a person that has been collected publicly ought to be subject to privacy limitations. This has given rise to a debate about the issue of "privacy in public"; a debate that is unfortunately beyond the scope of this paper to discuss.

The International Bill of Rights

The biggest problem with discussion of moral issues that arise in a medium like the Internet, is that there is little agreement about what moral theories ought to be applied to

such a discussion. One scholar might wish to discuss these issues in purely utilitarian terms, but such a discussion is unlikely to be well-received by another scholar who wishes to discuss that same issue in Kantian terms, and both are likely to disagree with yet another scholar who wishes to discuss the same issue in terms of an ethic of care. Such problems are only magnified by the global nature of the Internet; in order to come to any satisfactory answer to these problems, it is necessary to rely on some global, or near-global, theory of ethics.

There is really only one moral standard in the world today that fits with the global nature of the Internet, and that is the International Bill of Rights. Assented to by the General Assembly of the United Nations,[12] the International Bill of Rights consists of three documents: the Universal Declaration of Human Rights (UDHR), the International Covenant on Economic, Social and Cultural Rights (CESCR) and the International Covenant on Civil and Political Rights (CCPR). The International Bill of Rights was reaffirmed by 171 countries of the world at the World Conference on Human Rights, held in Vienna in June 1993. As of November 2, 2003, the United Nations consisted of 189 member states, so the reaffirmation of the UDHR by 171 nations represents the overwhelming majority of the nations (and peoples) of the world. Such international agreement to a common moral standard makes these human rights instruments an excellent tool for assessing the issues raised in the use of an international medium such as computing, and the Internet.

Both the UDHR and the CCPR assert that people have a right to privacy. Article 12 of the UDHR states that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[12] In fact, recognition and promotion of human rights is central to the mission of the United Nations, being mentioned in Article 1 of the United Nations Charter.

Article 17 of the CCPR is virtually identical:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The biggest difference between these two documents is that the UDHR is merely an aspirational document, whereas the CCPR is an international treaty, legally binding upon its signatories, who are thus committed to taking steps to ensure that the rights enumerated in the CCPR are incorporated into domestic law. As of November 2003, 151 nations had ratified this treaty, thus agreeing to be bound by its standards. Such international agreement gives good grounds for asserting that there is a widely recognized right to privacy, and suggests that an attempt to deal with the issue of privacy and the Internet ought to utilize the notion of such a right. I would also suggest that given its widespread international acceptance, any attempt to deal with practical problems of privacy on the Internet also ought to give due recognition to the International Bill of Rights, and its to interpretation, to which so many nations have agreed to be bound.

Justified Violations of Rights – The Use of Harmful Methods

The International Bill of Rights certainly does not propose an absolute right to privacy. Rather these declarations of rights are intended to protect persons against "arbitrary" interference with their privacy. So what does this actually mean? The Shorter Oxford Dictionary defines arbitrary as "Unrestrained in the exercise of will or authority; despotic, tyrannical."[13] Thus an arbitrary violation of privacy would be a violation that was based on an unrestrained exercise of authority, and a non-arbitrary violation of privacy would be a violation that was justified according to recognisable and objectively defined standards. In fact, many countries have recognised the need to establish clear standards that make it possible to clearly differentiate between justified and unjustified

[13]Brown, Lesley (Ed.) *The New Shorter Oxford English Dictionary (3rd Ed.)* (Oxford: Clarendon, 1993.)

violations of privacy, laying down in legislation the specific conditions that must be met in order for a violation of the right to privacy to be legal. The basis of these laws, as with most criminal laws, are ethical principles – so the laws themselves reveal the ethical principles that are considered to be important.

In order the determine when it might be justified to violate a particular person's right to privacy, it is necessary to have some understanding of when it is going to be generally justifiable to violate a right. The area of police ethics has been an important source of discussion in this area, since the violation of rights is an everyday occurrence in police-work. The basic principle in that area is that a police officer will only be justified in violating a person's moral rights if the following rules are met:

(1) The police officer is aiming to achieve a good end.

(2) The violation of rights is necessary - i.e. there are no other means that could be used to achieve this end.

(3) The good that is being aimed at by violating this right, outweighs the evil that will follow from violating the right – i.e. the violation of rights is proportional to the end that is being aimed at.

The usual situation where a police officer will be required to violate a particular person's rights, is where such a violation is necessary in order to protect the rights of another person. In order for condition (3) to be met, the rights that the police officer is aiming to protect would have to be at least as fundamental is the rights that the police officer is going to violate.

A practical example that illustrates this situation, is when a police officer is forced to resort to the use of deadly force. If a police officer is going to violate a person's right to life (or threaten to violate their right to life) through the use of deadly force, then this will only be considered to be proportional to the situation if the officer is using deadly force to protect the right to life of another person. One person's right to life is threatened by the police officer in order to protect the equally fundamental right of someone else. It can clearly be seen that the police officer would not be justified in using deadly force in order

to prevent a theft – the right to own property is not as fundamental as the right to life, thus it would not be proportional for a police officer to threaten to violate the right to life in order to protect another person's right to own property.

The three rules that I mentioned earlier are really the only justification for any violation of rights: in order for it to be justified for person A to violate any of the moral rights of person B, the three conditions must be met. Person A must be aiming at a good end, there must be no other way of achieving that end that does not violate rights, and the violation of the rights of person B must be proportional to the end that is being aimed at – i.e. the right that is being protected by violating the rights of person B must be at least as fundamental as the right of person B that is being violated. (In fact, in situations where these three conditions are actually met, it will often be the case that person B is attempting to violate the rights of another person, and that this is the reason why it is justified to violate the rights of person B).

There is one important general consequence of the need for justification for the violation of rights. Any time that an important moral right is being violated, if that violation of rights is to be considered justified, then the circumstances of that individual case will need to be examined. One cannot give a blanket approval for the violation of rights, each violation will have to be considered on a case-by-case basis to determine if that particular violation of rights is justified.

In order for it to be justified to violate any person's right to privacy, the three basic conditions must be met; good ends aimed at, privacy violation necessary, and privacy violation proportional to the ends aimed at. In general, it will only be justified to violate a person's right to privacy where this is necessary in order to preserve the more fundamental rights of others, rights such as life, liberty, and security of person.

The need to justify violations of the right to privacy has long been recognised in law. For example, if a police officer wants to violate a particular person's right to privacy, such as

by searching their house or by tapping their telephone, (and if the officer wishes to do this legally!) then it is necessary for the police officer to obtain a warrant. In order to get a warrant that will allow this legal invasion of privacy, the officer must provide evidence that this violation of privacy is justified, by showing that the violation is necessary and that there are reasonable grounds at law to allow the violation of rights. In effect, the officer is being asked to prove to a third party (usually a judge) that this particular violation of rights meets the three general rules for justified violation of rights.

In the terms of the International Bill of Rights, if a particular violation of privacy meets the three general conditions for the violation of rights, then that violation of the right is privacy is non-arbitrary, and invading someone's privacy in this way would not breach the right to privacy clauses of the UDHR or the CCPR.

Having discussed the arbitrary and non-arbitrary violation of the right to privacy, it is now time to return to the final task of this paper – to see what the International Bill of Rights might say about the issue of privacy, and how this might apply to issues of privacy arising from the Internet.

The Right to Privacy and the Internet

In discussing the International Bill of Rights, and its relation to the issue of privacy on the Internet, I will begin by examining the published comments of the Office of the High Commissioner for Human Rights (OHCHR) regarding the interpretation of article 17 of the CCPR, to see if some greater insight into the right to privacy can be gained in this way. Such comments are extremely important, since in agreeing to the CCPR, nations are binding themselves to the interpretation provided by the OHCHR.

There are eleven particular points raised in the OHCHR comment on article 17 of the CCPR. Of these, several are particularly relevant to the issue of privacy and the Internet. Point 3 notes that when the article prohibits "unlawful interference" with privacy, that this means that no interference with privacy can take place except for cases specifically authorised by law, and that the law itself must also comply with the provisions of the

covenant. Point 4 emphasises this even further, by noting that arbitrary interference is also prohibited by the covenant, and this may well include interference that is provided for under law. Any legal interference with privacy should be reasonable in the particular circumstances.

Point 8 deals specifically with correspondence, and notes that:

> Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

Point 8 also notes that where authorised interference with correspondence is contemplated, that such interference may only be made by the authority designated under the law, and that the decision to engage in such interference must be made on a case-by-case basis. Point 9 notes that state parties are also under an obligation not to engage in interference with correspondence that is inconsistent with article 17 of the covenant.

Point 10 deals with the gathering and holding of personal information in computer databases. Apart from stating that such activities must be regulated by law, it also states that individuals have the right to know who holds such databases, who has access to those databases, and what information is held about each individual in those databases. In the event that any information so held is found to be incorrect, or to have been gathered or processed contrary to law, then each individual is entitled to request rectification of the incorrect information, or elimination of the improperly collected information.

The comments made regarding the implications and implementation of article 17 gel nicely with the comments that I made earlier in this paper about circumstances where privacy may justifiably be breached. However, the comments have major implications in the area of privacy on the Internet, since they bear on many practices that have been

mentioned during the course of this paper.

In discussing "reasonable expectations of privacy" in Internet transactions, Robert McArthur noted that e-mail was an insecure medium, and thus suggested that there was no right to privacy in e-mail correspondence. Among the reasons that he gave for holding this view were the fact that e-mail was commonly monitored by employers, and that innocent e-mails were often intercepted by FBI software that attempts to target the e-mails of suspected criminals. I hope that this paper has shown that McArthur's position, while plausible legally, is certainly not plausible morally. The arbitrary monitoring of employees' e-mail is a violation of the employees' privacy, that fails to meet the three conditions necessary to justifiably violate this right. The monitoring of e-mail by the FBI is also a violation of the right to privacy, and is in fact specifically ruled out in the OHCHR comments regarding article 17 of the CCPR, which states that "the integrity and confidentiality of correspondence should be guaranteed". If e-mail was to be examined, then in order for this violation of the right to privacy to be justified, a decision regarding the interference would have to be made on a case-by-case basis; this is all too clearly not the situation with FBI monitoring of e-mail.

McArthur also discusses the issue of Internet companies collecting data about the browsing habits of users of the World Wide Web, and again suggests that there is no violation of privacy involved in such data collection. Again I would disagree, and would argue that not only is the collection of such data clearly an arbitrary violation of privacy, but also that the collection of such information without the express consent of the individual involved is also a significant breach of the individual's right to privacy.

Many other specific issues and Internet practices could be raised and discussed, but I believe that this is unnecessary. It is my hope that this paper has at least made clear some of the main problems with regard to the right to privacy and the Internet, and that I have managed to point out the wide number of ways that the privacy of users of the Internet might be unjustifiably be violated.